UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/402,144	09/29/1999	MARTINA HANCK	P991784	5593

29177 7590 08/22/2006

BELL, BOYD & LLOYD, LLC
P. O. BOX 1135
CHICAGO, IL 60690-1135

EXAMINER	
KIM, JUNG W	

ART UNIT	PAPER NUMBER
2132	

DATE MAILED: 08/22/2006

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/402,144	HANCK ET AL.	
	Examiner	Art Unit	
	Jung Kim	2132	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *01 August 2006*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-3,10-12,22-33 and 37-48* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-3,10-12,22-33 and 37-48* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☒ All b)☐ Some * c)☐ None of:

1.☒ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

KAMBIZ ZAND
PRIMARY EXAMINER

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

1. This Office action is in response to the amendment filed on August 1, 2006.

2. Claims 1-3, 10-12, 22-33 and 37-48 are pending.

Response to Arguments

3. On pg. 9, 5th paragraph of the Remarks, applicant alleges that Kilner teaches away from the use of a hashing value or a cryptographic one-way function and cites column 1, lines 41-55 of Kilner as evidence. However, applicant provides no explanation how the portion cited teaches away from using a hashing value or a cryptographic one-way function. The cited portion in question discusses deficiencies in two techniques of updating a database by locking a changed record until the change has been recorded or transferring the results of a change to a copy via a link; Kilner discloses these deficiencies are apparent when there are multiple changes to the same record, causing overhead under a heavy loading conditions. But nary a mention to teach away from the use of a hashing value or cryptographic one-way function in lieu of a CRC code. Hence, applicant's argument is not persuasive.

4. In reply to applicant's argument that "the CRC check performed in Kilner would not be properly combined with the teaching in Frezza, as the checksum operation on the booter data in Frezza would not be compatible with the CRC operation of Kilner," examiner respectfully disagrees. The checksum operation on the booter data is implemented in the same context as the CRC operation of Kilner. In both disclosures

the checksum operation and CRC are means to validate the integrity of the transmitted data values. Moreover, Frezza discloses motivation to encrypt the integrity of the checksum: to prevent unauthorized parties from infiltrating and controlling a communication network in which data is transmitted. (2:68-3:3) Hence, applicant's argument is not persuasive.

5. Applicant's remaining arguments are moot in view of the new rejections further in view of Renaud against the amended claims.

Claim Rejections - 35 USC § 103

6. Claims 1-3, 10, 22-33, 37, 40, 43 and 46 are rejected under 35 U.S.C. 103(a) as being unpatentable over Kilner USPN 5,649,089 in view of Renaud et al. USPN 5,958,051 (hereinafter Renaud) and Frezza et al. U.S. Patent No. 4,982,430 (hereinafter Frezza); subject matter in McNamara et al. USPN 4,533,948 is relied upon since the McNamara patent is incorporated by reference into the Frezza patent (hereinafter McNamara).

7. As per claim 10, Kilner discloses an arrangement for forming a first commutative checksum for digital data which are grouped into a number of data segments, the arrangement comprising:

a. an arithmetic and logic unit, (fig. 1, reference nos. 112 and 115)

b. a first segment checksum, which is formed for each said data segment, (fig. 1, reference no. 124)

c. a commutative operation which forms the first commutative checksum by operating on the segment checksums. (fig. 1, reference no. 130)

8. Kilner discloses forming the first segment checksum in accordance with a CRC (3:38) and Frezza discloses it is desirous to secure the integrity check of the data (ibid) but neither Kilner nor Frezza disclose forming the first segment checksum in accordance with a type selected from the group consisting of a hashing value and a cryptographic one-way function. Renaud discloses a method for implementing digital signatures for data streams wherein identifiers for files are generated to uniquely identify the files based on the original file without modification using a CRC or alternatively a one-way hash value. Renaud further discloses that a one-way hash provides more security over a CRC since the one-way hash cannot be easily reverse engineered. (7:15-28) Therefore, it would be obvious to one of ordinary skill in the art at the time the invention was made to form the first segment checksum in accordance with a type selected from the group consisting of a hashing value and a cryptographic one-way function. One would be motivated to do so to provide a more secure means of uniquely identifying the digital data as disclosed by Renaud, ibid.

9. Kilner does not cover a cryptographic operation to protect the first commutative checksum. Frezza teaches encrypting integrity values prior to submitting the integrity value over a network link to prevent unauthorized alteration of a message. Frezza, col. 2:45-3:13. It would be obvious to one of ordinary skill in the art at the time the invention was made to implement a cryptographic operation to secure the first commutative checksum. One would be motivated to do so to prevent an unscrupulous third party

from an unauthorized modification of a transmitted message (Frezza, col. 2:20-25). The aforementioned cover the limitations of claim 10.

10. As per claim 37, Kilner in view of Renaud and Frezza cover the following: 1) an arrangement for forming a first commutative checksum, 2) an arrangement for checking a predetermined cryptographic commutative checksum, and 3) an arrangement for forming and checking a first commutative checksum as outlined above in the claim 10 rejection 35 U.S.C. 103(a). In addition, the cryptographic operations described use a symmetric key methodology (Frezza, col. 1:12-19; 5:50-58; McNamara, 7:34-42; 8:25-35).

11. As per claims 40, Kilner in view of Renaud and Frezza cover the following: 1) an arrangement for forming a first commutative checksum, 2) an arrangement for checking a predetermined cryptographic commutative checksum, and 3) an arrangement for forming and checking a first commutative checksum as outlined above in the claim 10 rejection under 35 U.S.C. 103(a). In addition, Kilner teaches the commutative operation to establish column parity, which forms the commutative checksums, is an XOR operation (Kilner, col. 3:52-65): the XOR operation exhibits both commutative and associative properties. The aforementioned cover the limitation of claim 40.

12. As per claim 43, Kilner in view of Renaud and Frezza cover an arrangement as outlined above in the claim 10 rejection under 35 U.S.C. 103(a). Kilner does not

expressly disclose archiving the digital data and the cryptographic commutative checksum. However, archiving the elements of a transmission is a standard feature to verify the contents of a transmission to an auditor. The examiner takes Official Notice that archiving transmission elements are standard means to record the transmission to prove the contents and status of the transmission at a latter date (i.e. auditing a transmission). It would be obvious to one of ordinary skill in the art at the time the invention was made to archive the digital data and the checksum since it preserves a receipt of the transmission. The aforementioned cover the limitations of claim 43.

13. As per claim 46, Kilner in view of Renaud and Frezza cover the following: 1) an arrangement for forming a first commutative checksum, 2) an arrangement for checking a predetermined cryptographic commutative checksum, and 3) an arrangement for forming and checking a first commutative checksum as outlined above in the claim 10 rejections under 35 U.S.C. 103(a). In addition, as mentioned previously, the digital data is cryptographically protected, and by convention, the cryptographic operation would be implemented by an ALU. Furthermore, since Kilner discloses sending the digital data as well as the checksum values and commutative checksum value from the active database to a standby database over a network link (col. 3:14-19, and figs.1-4), and Frezza teaches securing the integrity value being transmitting over a digital network, the digital data would necessarily be processed in accordance with a network management protocol. The aforementioned cover the limitation of claim 46.

14. As per claims 1-3 and 22-33, they are method claims corresponding to the subject matter covered in the rejections of claims 10, 37, 40, 43 and 46, and they do not teach or define above the information covered in the rejections of claims 10, 37, 40, 43 and 46. Therefore, claims 1-3 and 22-33 are rejected under Kilner in view of Renaud and Frezza for the same reasons set forth in the rejections of claims 10, 37, 40, 43 and 46.

15. Claims 11, 12, 38, 39, 41, 42, 44, 45, 47 and 48 are rejected under 35 U.S.C. 103(a) as being unpatentable over Kilner in view of Renaud and Frezza (the subject matter of McNamera is dependent upon since McNamera is incorporated by reference into the Frezza patent), and further in view of Mattison USPN 5,778,070 (hereinafter Mattison).

16. As per claim 11, Kilner in view of Renaud and Frezza cover an arrangement as outlined above in the claim 10 rejection under 35 U.S.C. 103(a). In addition, the arrangement also includes the following:

d. the allocation of the predetermined cryptographic checksum to the digital data and the subjection of the cryptographic commutative checksum to an inverse cryptographic operation to form a first commutative checksum (Frezza, col. 1:12-19; 5:50-58; McNamara, 7:34-42; 8:25-35; any message encrypted by DES has an inverse operation (decryption) to retrieve the original message; furthermore, every ciphertext is associated with a specific plaintext);

e. the formation of a second segment checksum for each data segment, the formation of a second commutative checksum by a commutative operation on the second segment checksums, and a comparison of the first commutative checksum and the second commutative checksum for a match (Kilner, 4:10-26).

17. Kilner discloses the first segment checksum is formed in accordance with a CRC (3:38) and Frezza discloses it is desirous to secure the integrity check of the data (ibid) but neither Kilner nor Frezza disclose the first segment checksum is formed in accordance with a type selected from the group consisting of a hashing value and a cryptographic one-way function. Renaud discloses a method for implementing digital signatures for data streams wherein identifiers for files are generated to uniquely identify the files based on the original file without modification using a CRC or alternatively a one-way hash value. Renaud further discloses that a one-way hash provides more security over a CRC since the one-way hash cannot be easily reverse engineered. (7:15-28) Therefore, it would be obvious to one of ordinary skill in the art at the time the invention was made for the first segment checksum to be formed in accordance with a type selected from the group consisting of a hashing value and a cryptographic one-way function. One would be motivated to do so to provide a more secure means of uniquely identifying the digital data as disclosed by Renaud, ibid.

18. Kilner does not teach the second segment checksum is formed in accordance with a type selected from the group consisting of a hashing value and a cryptographic one-way function. However, the use of a hashing value as a checksum is a well known means to ensure the integrity of a data segment. For example, Mattison discloses

hashing as a more rigorous means than a typical checksum to ensure data integrity since a hash of a data block is unique to that data block and any modification to the data block will modify the hash (5:20-34). Therefore, it would be obvious to one of ordinary skill in the art at the time the invention was made for the segment checksum to be a hashing value. One would be motivated to do so to establish a more rigorous integrity check on the data segments. The aforementioned cover the limitations of claim 11.

19. As per claim 12, since the second segment checksum (the checksum to verify an integrity value) is a hash value, the first segment checksum (the checksum to form an integrity value) is also a hash value. Hence, the above arrangements outlined in the claim 10 and 11 rejections under 35 U.S.C. 103(a) together covers the arrangement outlined in claim 12.

20. As per claims 38 and 39, Kilner in view of Renaud, Frezza and Mattison cover the following: 1) an arrangement for forming a first commutative checksum, 2) an arrangement for checking a predetermined cryptographic commutative checksum, and 3) an arrangement for forming and checking a first commutative checksum as outlined above in the claim 11 and 12 rejections under 35 U.S.C. 103(a). In addition, the cryptographic operations described use a symmetric key methodology (Frezza, col. 1:12-19; 5:50-58; McNamara, 7:34-42; 8:25-35).

21. As per claims 41 and 42, Kilner in view of Renaud, Frezza and Mattison cover the following: 1) an arrangement for forming a first commutative checksum, 2) an arrangement for checking a predetermined cryptographic commutative checksum, and 3) an arrangement for forming and checking a first commutative checksum as outlined above in the claim 11 and 12 rejections under 35 U.S.C. 103(a). In addition, Kilner teaches the commutative operation to establish column parity, which forms the commutative checksums, is an XOR operation (Kilner, col. 3:52-65): the XOR operation exhibits both commutative and associative properties. The aforementioned cover the limitations of claims 41 and 42.

22. As per claims 44 and 45, Kilner in view of Renaud, Frezza and Mattison cover an arrangement as outlined above in the claim 11 and 12 rejections under 35 U.S.C. 103(a). Kilner does not expressly disclose archiving the digital data and the cryptographic commutative checksum. However, archiving the elements of a transmission is a standard feature to verify the contents of a transmission to an auditor. The examiner takes Official Notice that archiving transmission elements are standard means to record the transmission to prove the contents and status of the transmission at a latter date (i.e. auditing a transmission). It would be obvious to one of ordinary skill in the art at the time the invention was made to archive the digital data and the checksum since it preserves a receipt of the transmission. The aforementioned cover the limitations of claims 44 and 45.

23. As per claims 47 and 48, Kilner in view of Renaud, Frezza and Mattison cover the following: 1) an arrangement for forming a first commutative checksum, 2) an arrangement for checking a predetermined cryptographic commutative checksum, and 3) an arrangement for forming and checking a first commutative checksum as outlined above in the claim 11 and 12 rejections under 35 U.S.C. 103(a). In addition, as mentioned previously, the digital data is cryptographically protected, and by convention, the cryptographic operation would be implemented by an ALU. Furthermore, since Kilner discloses sending the digital data as well as the checksum values and commutative checksum value from the active database to a standby database over a network link (col. 3:14-19, and figs.1-4), and Frezza teaches securing the integrity value being transmitting over a digital network, the digital data would necessarily be processed in accordance with a network management protocol. The aforementioned cover the limitations of claims 47 and 48.

Conclusion

Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not

mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

Communications Inquiry

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Jung W. Kim whose telephone number is 571-272-3804. The examiner can normally be reached on M-F 9:00-5:00.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gilberto Barron can be reached on 571-272-3799. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

KAMBIZ ZAND
PRIMARY EXAMINER

JK
Jung W Kim
Examiner
AU 2132
8/18/06